UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/918,602	07/30/2001	Christopher P. Jalbert	04860P2441	5216

7590 01/13/2005

James C. Sheller
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER	
SCHUBERT, KEVIN R	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 01/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/918,602	JALBERT ET AL.	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 July 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *07302001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-41 have been considered.

Claim Objections

Claim 11 is objected to because of the following informalities: the phrase "each subsequent combining functions" in part c) should be replaced by the phrase "each subsequent combining function". Appropriate correction or clarification is required.

Claim 36 is objected to because of the following informalities: the examiner believes the phrase "as applied" should be "is applied". Appropriate correction or clarification is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 16 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention. In part b) the applicant refers to "the received signal". It is unclear which received signal the applicant is referring to. The examiner will assume "the received signal" refers to the signal received at the second entity which is the random nonce encrypted with the secret. Appropriate clarification is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-13,16-17,19-23 are rejected under 35 U.S.C. 102(b) as being anticipated by Vogelesang, U.S. Patent No. 5,953,424.

As per claims 1,20, and 21, the applicant claims a cryptographic method with the following limitations which are met by Vogelesang:

a) receiving at a first entity a second public key M_A (Col 16, lines 33-38);

b) generating at least one of a first session key K_B and a first secret S_B based on the second public key M_A (Col 16, lines 39-42);

c) generating a first random nonce N_B (Col 16, lines 64-67);

d) encrypting the first random nonce N_B with at least one of the first session key K_B and the first secret S_B to obtain an encrypted random nonce (Col 16, lines 64-67);

e) transmitting the encrypted random nonce from the first entity (Col 16, lines 64-67);

f) in response to transmitting the encrypted random nonce, receiving at the first entity a data signal containing a modification of the first random nonce $N_B + 1$ (Col 17, lines 19-24);

g) if the received modification of the first random nonce $N_B + 1$ was correctly performed then performing at least one of

i) opening a communication link at the first computer and

ii) generating a first initialization vector I_B (Col 17, lines 25-37);

Vogelesang describes an authentication method like the applicant's which seeks to prevent man in the middle attacks. Mutual entity authentication between the two parties is done in the preferred embodiment according to a shared secret S.

Regarding part a), either the first participant or the second participant could be deemed the first entity and either X or Y could be deemed the second public key in the example. The examiner will consider the first participant to be the first entity and the second public key to be Y. The applicant should note that the formula for Y is identical to the formula for M_A.

Regarding part b), the shared secret S is the secret S_B which the first participant generates using Y, or the second public key.

Regarding parts c),d), and e), the random nonce is the private signal L which is encrypted with the secret and passed to the second participant.

Regarding part f), the second participant adds one to L to get M and sends M, or L + 1, back to the first participant.

Regarding part g), the example is given to show how the first entity authenticates the second entity. Once authentication has taken place the first entity, which is a computer in the preferred embodiment since the invention takes place between two computer systems (Col 1, lines 6-9), opens an authenticated communication link.

Regarding claims 20 and 21, the use of "computer readable storage" (claim 20) and a "distributed readable storage medium containing executable computer program instructions" (claim 21) is met by Vogelesang because the invention takes place within "computer systems" (Col 1, lines 8-9).

As per claim 2, the applicant describes the method of claim 1, which is met by Vogelesang (see above), with the following limitation which is also met by Vogelesang:

Determining whether the received modification was correctly performed (Col 17, lines 25-37).

As per claim 3, the applicant describes the method of claim 2, which is met by Vogelesang (see above), with the following limitation which is also met by Vogelesang:

Wherein determining whether the received modification was correctly performed includes checking whether the received modification of the first random nonce $N_B + 1$ equals a modification of the first random nonce $N_B + 1$ as applied to the first random nonce $N_B + 1$ by the first entity (Col 17, lines 25-37).

As per claim 4, the applicant describes the method of claim 2, which is met by Vogelesang (see above), with the following limitation which is also met by Vogelesang:

Wherein determining whether the received modification was correctly performed includes checking whether the received modification of the first random nonce $N_B + 1$ less a modification thereof as applied thereto by the first entity equals the first random nonce $N_B + 1$ (Col 17, lines 25-37).

As per claim 5, the applicant describes the method of claim 1, which is met by Vogelesang (see above), with the following limitation which is also met by Vogelesang:

Wherein generating the first session key K_B includes

a) presenting a number parameter B_B (Col 16, lines 39-40);

b) generating a first random number R_B (Col 16, lines 39-40);

c) setting the first session key K_B equal to the second public key M_A raised to the exponential power of the first random number R_B, modulo parameter B_B (Col 16, lines 39-42);

The applicant should note that the secret key is a session key and that the secret key can take many forms. Parameter B_B is n, random number R_B is A, and the public key M_A is Y. Note that factors K and J, which are used some of the time depending on whether they are present in the system, are also included in this form of the equation.

As per claim 6, the applicant describes the method of claim 1, which is met by Vogelesang (see above), with the following limitation which is also met by Vogelesang:

Wherein generating the first secret S_B includes employing a combining function, f_B (Col 8, lines 7-10);

Again, the applicant should note that the secret can take many forms. This combining function in the lines referenced above is just one possibility.

As per claim 7, the applicant describes the method of claim 6, which is met by Vogelesang (see above), with the following limitation which is also met by Vogelesang:

Wherein employing the combining function, f_B, includes first generating a first public key M_B, the combining function, f_B, then being employed on a first password P_B and on at least one of the second public key M_A and the first public key M_B (Col 8, lines 7-10);

In the example referenced above, K is the authentication factor, which can be a password (Col 8, lines 41-42). Since the secret is a combining function of a modification of the first public key Y (M_B) and the password, the claim is satisfied. Also, the applicant should note that the lines referenced above (Col 8, lines 7-10) present just one example and the invention is applicable to a combining function of the unmodified public key Y (M_B) and the password.

As per claim 8, the applicant describes the method of claim 7, which is met by Vogelesang (see above), with the following limitation which is also met by Vogelesang:

Wherein employing the combining function, f_B, on a first password P_B and on at least one of the second public key M_A and the first public key M_B includes

The applicant should note that in the example the combining function hashes a modified second public key Y (M_A) with password K (P_B) and the additional factors J and H, which are what you have factors. The first public key (M_B) is a what you have factor and could be J, and H does not have to appear if the system does not have or want to use another what you have factor. Thus, the hash of modified second public key, password, and first public key is presented in the example. The applicant should also note that another example representing the hash of an unmodified second public key, password, and first public key is encompassed by the invention.

As per claim 9, the applicant describes the method of claim 8, which is met by Vogelesang (see above), with the following limitation which is also met by Vogelesang:

Wherein the secure hash is a one-way hash function (Col 8, lines 14-23);

The applicant should note that the hash algorithms listed in the lines referenced above are known to be used mainly as one-way hash functions.

As per claim 10, the applicant describes the method of claim 9, which is met by Vogelesang (see above), with the following limitation which is also met by Vogelesang:

Wherein the one-way hash function is one of the Secure Hash Algorithm, the Message Digest 5, Snefru, Nippon Telephone and Telegraph Hash, and the Gosudarstvennyl Standard (Col 8, lines 14-23);

As per claim 11, the applicant describes the method of claim 6, which is met by Vogelesang (see above), with the following limitation which is also met by Vogelesang:

Wherein employing the combining function, f_B, includes employing a plurality of combining functions to produce the first secret S_B, wherein each of the plurality of combining functions produces a prior result, wherein employing a first combining function includes

a) generating a first public key M_B (Col 10, line 40);

b) employing the first combining function on a first password P_B and on at least one of the second public key M_A and the first public key M_B (Col 10, line 40);

c) employing each subsequent combining functions includes employing a combining function on a prior result and on at least one of the second public key M_A, the first password P_B, and the first public key M_B, wherein the prior result produced by the last combining function is the first secret S_B (Col 10, line 40);

The hash as illustrated in the line referenced above is a combining hash of the components (Col 10, line 56). Furthermore, if the expression with only Y (or M_A), K (or P_B), and J (or M_B) is used, a prior result would be combining the expression of Y (or M_A) with K (or P_B). This expression would then be combined with J (or M_B) in the hash to produce the secret S (or S_B).

As per claim 12, the applicant describes the method of claim 6, which is met by Vogelesang (see above), with the following limitation which is also met by Vogelesang:

Wherein encrypting the first random nonce N_B includes employing a symmetrical encryption algorithm (Col 16, lines 64-67; Col 9, lines 44-50);

The applicant should note that the secret S (S_B) which is used to encrypt the first random nonce L in the example is a symmetrical encryption algorithm (Col 9, lines 44-50).

As per claim 13, the applicant describes the method of claim 12, which is met by Vogelesang (see above), with the following limitation which is also met by Vogelesang:

Wherein the symmetrical encryption algorithm is one of the Data Encryption Standard and the block cipher CAST (Col 1, lines 59-61);

Use of the DES is referenced in the Background as a standard for use in the disclosed invention.

As per claim 16, the applicant describes the method of claim 1, which is met by Vogelesang (see above), with the following limitation which is also met by Vogelesang:

a) wherein transmitting the encrypted random nonce from the first entity includes transmitting a first public key M_B (Col 16, lines 64-67);

b) wherein the received signal is encrypted based on at least one of a second session key K_B and a second secret S_B (Col 16, lines 64-67; Col 17, lines 19-24);

c) wherein the second session key K_B and the second secret S_B are based on the first public key M_B (Col 16, lines 39-42);

Regarding part a), the applicant should note that the random nonce is encrypted by S which is a function of the first public key, so transmitting the encrypted random nonce includes transmitting the first public key. Proper decryption can reveal both the first public key and the random nonce.

Regarding part b), the received signal is encrypted according to the secret S (S_B).

Regarding part c), the secret S is based on the first public key Y (M_B). Since the secret key is the session key in Vogelesang's system, the session key is also based on the first public key Y (M_B).

As per claim 17, the applicant describes the method of claim 1, which is met by Vogelesang (see above), with the following limitation which is also met by Vogelesang:

Wherein the signal further includes a second random nonce N_A and wherein, subsequent to generating the first initialization vector I_B, the method further including:

a) modifying the second random nonce N_A to obtain a modified second random nonce N_{AB} + 1 (Col 13, lines 64-67);

b) encrypting the modified second random nonce N_{AB} + 1 with at least one of the first session key K_B and the first secret S_B to obtain an encrypted package (Col 14, lines 1-4);

c) transmitting the encrypted package from the first computer (Col 14, lines 1-2);

d) in response to transmitting the encrypted random nonce, receiving at the first computer a request to open a communication channel (Col 14, lines 2-4);

e) opening the communication channel (Col 14, lines 2-4);

The example referenced above is used to show how two entities who do not have the proper secret cannot establish authentication between themselves. However, the method of mutual authentication through two nonces (though it was used for an illustration of the importance of the secret) can be used to meet the limitations of the claim. The L is the first nonce used to authenticate the second party. The V is the second nonce used to authenticate the first party.

Regarding claims d) and e), if the entities are authenticated (which is not the case in the example because of the secret), then authenticated communication takes place.

As per claim 19, the applicant describes the method of claim 17, which is met by Vogelesang (see above), with the following limitation which is also met by Vogelesang:

Wherein the communication channel is a two-way communication channel (Col 13, lines 41-67; Col 14, lines 1-4);

Since the example demonstrates mutual entity authentication through nonces L and V, a two-way authentication process takes place which leads to a two-way communication channel being opened up.

As per claim 22, the applicant describes a computer system, which has limitations d) through j) which are met by claim 1, and the following additional limitations which are also met by Vogelesang:

a) a processor (Col 1, lines 6-9);

b) a network interface coupled to the network and coupled to the processor, the network interface receiving a page request including information on at least one of a user identification and a user password (Col 11, lines 53-61);

c) a file storage device coupled to the processor, the file storage device storing copies of at least one of a user identification and a user password under control of a file management system, and wherein the processor performs a method (Col 11, lines 53-61);

The applicant should note that the use of a processor is met because the system takes place within an environment of computer systems, which have processors.

As per claim 23, the applicant describes the computer system of claim 22, which is met by Vogelesang (see above), with the following limitation which is also met by Vogelesang:

Wherein the network may be a network operating according to a hypertext transfer protocol (Col 1, lines 12-14);

The applicant should note that Vogelesang references the Internet, and hypertext transfer protocol is a set of rules for transferring files on the Internet.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 24-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang in view of Kaufman, U.S. Patent No. 5,666,415.

As per claims 24,38, and 39, the applicant describes a cryptographic method with the following limitations which are met by Vogelesang in view of Kaufman:

a) receiving at a first entity a second public key M_A and a second random number N_A encrypted with a second password P_A (Kaufman: Col 3, lines 51-59);

b) generating at least one of a first session key K_B and a secret S_B based on the second public key M_A (Vogelesang: Col 16, lines 39-42);

c) employing a first password P_B to retrieve the second random number N_A from the second random number N_A encrypted with the second password P_A (Kaufman: Col 3, lines 51-59; Col 4, lines 14-18);

d) modifying the second random number N_A to obtain a modified second random number $N_A + 1$ (Vogelesang: Col 13, lines 41-57);

e) encrypting the modified second random number $N_{AB} + 1$ with at least one of the first session key K_B and the first secret S_B to obtain an encrypted random package (Vogelesang: Col 13, lines 41-57);

f) transmitting the encrypted random package from the first entity (Vogelesang: Col 13, lines 55-57);

g) in response to transmitting the encrypted random package, at least one of

i) receiving at the first entity a request to open a communication link

ii) receiving at the first entity an encrypted data package (Vogelesang: Col 13, lines 58-67; Col 14, lines 1-4);

As opposed to claim 1, claims 24,38, and 39, deal with a second embodiment of the applicant's invention in which the first entity initially receives a random number with the public key instead of just receiving the public key. This is done so that the second entity has the first opportunity to authenticate and/or cut off communication with the first entity. Kaufman describes an authentication similar to Vogelesang's in which a first entity, server, initially receives a password encrypted nonce. The password from a database is then used to obtain the random number.

The mutual entity authentication example described by Vogelesang (Col 13, lines 41-67; Col 14, lines 1-4) provides the framework where two nonces (L and V) are used in the mutual authentication. Lastly, in regards to part g), the encrypted random package sent from the first entity includes N, a modification of L used to verify the first entity, and V, used to verify the second entity. In response, the

second entity sends the first entity back a second encrypted data package which includes W, a modification of V, used to verify the second entity (Col 14, line 1).

The additional feature of having a random number encrypted by a password sent, as described by Kaufman, along with the public key is an obvious enhancement of Vogelesang's system because it allows the second entity to have the first opportunity to authenticate the first entity. Thus, it would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Kaufman with those of Vogelesang and incorporate sending a nonce along with the public key so the second entity has the first opportunity to authenticate.

Regarding claims 38 and 39, the use of "computer readable storage" (claim 38) and a "distributed readable storage medium containing executable computer program instructions" (claim 39) is met by Vogelesang because the invention takes place within "computer systems" (Col 1, lines 8-9).

As per claims 25-33,35-37, and 40-41, the claims recite limitations which have already been discussed above but are rejected under 35 U.S.C. 103(a), and not 102(b), because they depend on claims which are satisfied by Vogelesang in view of Kaufman.

For a discussion of the reasons for the rejection of claims 25 and 33, see claim 14.

For a discussion of the reasons for the rejection of claims 26-32 see claims 5-11 respectively. Accordingly, claim 26 is met by claim 5, claim 27 is met by claim 6,....., and claim 32 is met by claim 11.

For a discussion of the reasons for the rejection of claims 35-37 see claims 2-4 respectively. Accordingly, claim 35 is met by claim 2, claim 36 is met by claim 3, and claim 37 is met by claim 4.

For a discussion of the reasons for the rejection of claims 40-41, see claims 22-23 respectively. Accordingly, claim 40 is met by claim 22, and claim 41 is met by claim 23.

As per claim 34, the applicant describes the method of claim 24, which is met by Vogelesang in view of Kaufman, with the following limitation which is met by Vogelesang:

a) generating a first random number N_B (Col 13, line 54);

b) wherein encrypting the modified second random number N_{AB} + 1 includes encrypting as a first data signal the first random number N_B and the modified second random number N_{AB} + 1 (Col 13, lines 53-57);

c) and wherein receiving at the first computer an encrypted data package includes receiving a second data signal encrypted to at least one of a second session key K_A and a second secret S_A, the second data signal including a second initialization vector I_A and a modified first random nonce N_B + 1 (Col 13, lines 58-67; Col 11, lines 1-9);

d) retrieving the modified first random nonce N_B + 1 from the encrypted data package (Col 13, lines 58-67);

e) if the retrieved modification of the first random nonce N_B + 1 less was correctly performed then sending from the first entity a request to open a two way communication channel (Col 13, lines 58-67; Col 14, lines 1-4);

In regards to parts a),b), and c), the first random number N_B is V and the modified second random number N_{AB} + 1 is N. Both the first and second random numbers N and V are encrypted with the secret (Col 13, line 56) and sent to the first entity.

In regards to parts d) and e), N is received and decrypted at the first entity to compare its value with the value of L + 1 to authenticate the second entity. If the second entity is authenticated, a request to open a two way communication channel is sent via an encryption of W, a modification of first random number V, so that the second entity can authenticate the first entity. If this happens, both entities have been authenticated and a two way communication channel is opened for authenticated communication.

Claims 14-15 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang.

As per claims 14-15, the applicant describes the method of claims 6 and 14, which are met by Vogelesang (see above), with the following limitation:

Wherein encrypting the first random nonce N_B includes superencrypting the first random nonce N_B;

The use of superencryption is not considered a novel feature of the applicant's system. Though the use of superencryption is not describes by Vogelesang, it would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate superencryption as an added security enhancement.

As per claim 18, the applicant describes the method of claim 17, which is met by Vogelesang (see above), with the following limitation:

Wherein encrypting the modified second random nonce $N_{AB} + 1$ includes encrypting it with the first initialization vector I_B (Col 10, lines 63-67; Col 11, lines 1-9);

The use of encrypting with an initialization vector is described by Vogelesang though its implementation is not specifically cited within the patent. It would have been obvious to incorporate encrypting the second random nonce with the first initialization vector into Vogelesang's system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER